

Appl. No. : 09/712,398  
Filed : November 14, 2000

### REMARKS

Reconsideration and allowance of the above-referenced application is respectfully requested.

Initially, a number of the claims are canceled and/or narrowed herewith, in order to narrow the issues.

Claims 1, 2, 6, 7 and 15-17 stand rejected under 35 U.S.C. 102 as allegedly being unpatentable over Applebaum. Claims 1 and 2 has been canceled, with claims 3 and 7 being amended into independent form. Claims 15-17 have also been canceled to obviate the rejections thereto. The remaining rejections are respectfully traversed.

In rejecting claim 7, the rejection states that Applebaum teaches a limited exception mode that is operable without establishing that the personal information agrees with the decrypted information; referencing pages 8-9 and claim 36. However, this contention is respectfully traversed. Claim 36 states that the identification information is compared against the personal information, and that access is allowed if the personal information matches the identification information; and access is restricted of the personal information does not match. Nowhere is there any teaching or suggestion of a "limited exception mode without establishing that said personal information agrees with said decrypted information". Claim 36 of Applebaum simply states restricting the access the personal information does not match; and teaches nothing about such a limited exception mode, as claimed.

Therefore, claim 7 is completely patentable over Applebaum, and should be allowable for these reasons.

Claim 8 is rejected over Brody. This contention is respectfully traversed. Claim

Appl. N . : 09/712,398  
Filed : N vember 14, 2000

8 recites requesting a computer system to install a program and determining whether the program is verified for installation. Claim 8 recites obtaining "a reference biometric at the time of installing the software responsive to said determining...".

Therefore, this claim requires : a) determining whether the program is verified, and responsive to that determining, 2) obtaining a reference biometric. Therefore, any user can install the software, but, whoever that user is, they must give the program a reference biometric at the time of installation. After installing, claim 8 recites that the program is allowed "to run normally only when biometric information is obtained which matches said reference biometric".

This is a very different system than that disclosed by Brody. Brody requires that each piece of software is "individually personalized for each customer separately to include personal information of the customer..." see for example paragraph 147 of Brody. Nowhere is there any teaching or suggestion of obtaining this information as part of the installation routine. Rather, Brody requires that each copy of the software is individually personalized. This is a very difficult system, since it may very well be difficult to mass-market software which has been individualized in this way.

Brody admittedly teaches encryption and decryption in paragraph 152. However, note that the information is authenticated "prior to or during the software build". The verification of the personalization is at run time, but the individualization is carried out during the software build, see generally the beginning of paragraph 152.

Therefore, this system only allows installation of the software by the person for whom the software was personalized. In contrast, claim 8 allows anyone to install the software. However, once installed, the software is matched with a reference biometric,

**Appl. No.** : 09/712,398  
**Filed** : November 14, 2000

and cannot later be used by anyone who does not match the reference biometric. This produces advantages over Brody, and is nowhere taught or suggested by Brody.

Claim 9 is even further allowable, as it requires determining if the specified license has already been used. This would appear to be unnecessary in Brody who personalizes each copy of the program. Similar arguments apply for claim 10.

In rejecting claim 10, the rejection points attention to paragraphs like paragraphs 10 and 15 which describe how the prior art has recorded a unique serial number. However, Brody teaches personalizing each copy of the software, and therefore effectively teaches away from using such a unique serial number. Admittedly, Brody teaches finding and generating a unique identifier, but teaches nothing about using this to install the software so that the user's biometric information can be obtained at the time that the software is installed, as claimed.

Claim 19 was also rejected based on Brody. It is noted that Brody teaches using the personalization to determine whether the software can be installed, not whether it can be run after installation. Claim 19 specifies allowing the program to run in a specified way only when the reference biometric matches the current biometric. This is nowhere taught or suggested by Brody who only teaches verifying the information stream during installation, not at run time. The rejection refers to paragraph 153 as allegedly describing allowing the program to run in the specific way only when the reference biometric matches the current biometric. Paragraph 153 of Brody, however, teaches a different signature technique for the personal information. Paragraph 153 describes that this is detected "at run time" which, as emphasized throughout the remainder of Brody (e.g. C. paragraphs 147 and 152), refers to the time of installation.

**Appl. No.** : **09/712,398**  
**Filed** : **November 14, 2000**

Claim 3 has been amended into independent form, and was rejected over Applebaum in view of Brody. Applebaum does not teach a very different system than Brody, since Applebaum allows access to an appliance, not to a computer program. Applebaum teaches that biometric information can be obtained from the user and compared with biometric data that is stored to verify the identity. Paragraph 56 describes that encryption can be used. The encryption is described as being used to avoid the identity of the user being broadcast throughout the network. Other encryption is described in paragraphs 54 and 55.

Paragraph 54 describes that the encryption is carried out using the private key held by the server and that a public-key is provided to each user. However, nowhere is there any teaching or suggestion of doing this with a computer program, or any of the advantages that would be obtained from doing this with a computer program. Therefore, the hypothetical combination of these references is based on hindsight, and not on the teaching that the references define.

Claims 18 and 20 have been cancelled to obviate the rejection over Applebaum in view of Shinzaki.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the

Appl. No. : 09/712,398  
Filed : November 14, 2000

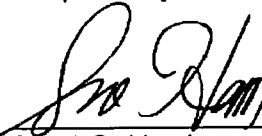
amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Therefore, and in view of the above amendments and remarks, all of the claim should be in condition for allowance. A formal notice to that effect is respectfully solicited.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387.

Respectfully submitted,

Date: 5/24/04

  
\_\_\_\_\_  
Scott C. Harris  
Reg. No. 32,030

Customer No. 23844  
Scott C. Harris, Esq.  
P.O. Box 927649  
San Diego, CA 92192  
Telephone: (619) 823-7778  
Facsimile: (858) 678-5082